

Compte rendu B1 TP21 : Création d'un scénario Linux

Sommaire

Introduction	1
1) La présentation du scénario (L'histoire détaillée)	2
2) Réponses à chacune des questions, avec en plus une capture d'écran,	3
Conclusion	6

Introduction

Ce TP a pour but de découvrir et d'utiliser les principales commandes Linux à travers un scénario professionnel. L'entreprise fictive **Cyber-Shield** doit préparer un environnement de travail sécurisé pour une mission d'audit bancaire. Ce travail permet d'apprendre à gérer les fichiers, les utilisateurs, les droits d'accès et les sauvegardes sur un système Linux.

1) La présentation du scénario (L'histoire détaillée)

Mon entreprise « **Cyber-Shield** », spécialisée dans l'audit de sécurité informatique pour les banques, doit mettre en place un nouvel environnement pour ses tests d'intrusion.

Je dois donc demander à l'administrateur système de tout d'abord passer en super utilisateur avec la commande su -. Pour vérifier que l'on soit bien le super utilisateur, on utilise la commande whoami, qui doit nous afficher « root ».

Il doit vérifier son emplacement actuel avec la commande pwd pour s'assurer qu'il est bien positionné. Il utilise ensuite la commande tree /home pour visualiser l'arborescence actuelle des dossiers des consultants.

L'administrateur doit créer un répertoire de travail pour la mission « Banque_X » avec la commande mkdir /home/mission_banque. Il entre dans ce dossier avec cd /home/mission_banque et crée un fichier de journalisation vide avec la commande touch logs.txt.

Pour remplir ce fichier, il utilise l'éditeur vim logs.txt. Il appuie sur la touche i pour insérer le texte « Audit_Demarré=Vrai », puis appuie sur Echap et tape :wq pour enregistrer et quitter. Il vérifie le contenu du fichier avec la commande cat logs.txt.

Par sécurité, il effectue une copie de ce fichier avec cp logs.txt logs.bak, puis il décide de renommer le fichier original avec la commande mv logs.txt rapport_final.log. Il finit par supprimer la copie devenue inutile avec rm logs.bak.

L'administrateur va maintenant créer l'utilisatrice « Johanne » avec la commande useradd johanne et lui attribuer un mot de passe avec passwd johanne. Il crée ensuite le groupe d'auditeurs avec groupadd auditeurs et y ajoute l'utilisatrice avec la commande usermod -aG auditeurs johanne.

Il doit sécuriser le rapport d'audit. Il change le propriétaire avec chown johanne rapport_final.log et le groupe avec chgrp auditeurs rapport_final.log. Pour que seule la propriétaire puisse modifier le fichier et le groupe seulement le lire, il tape la commande chmod 640 rapport_final.log. Il vérifie les droits avec ls -l rapport_final.log.

Pour sauvegarder le travail, il compresse le dossier de la mission avec la commande tar -czvf mission.tar.gz /home/mission_banque.

S'il remarque qu'un processus d'analyse est bloqué, il utilise ps aux | grep vim pour trouver le numéro du processus (PID), puis il l'arrête de force avec la commande kill -9 [PID]. Enfin, il affiche l'intégralité de ses actions pour vérification avec la commande history.

2) Réponses à chacune des questions, avec en plus une capture d'écran,

Question 1 : Passer en super utilisateur *Commande* : su -

```
romain@romain:~$ su -
Mot de passe :
[root@romain ~]#
```

Question 2 : Vérifier l'identité (root) *Commande* : whoami

```
[root@romain ~]# whoami
root
[root@romain ~]#
```

Question 3 : Vérifier l'emplacement actuel *Commande* : pwd

```
[root@romain ~]# pwd
/root
[root@romain ~]#
```

Question 4 : Visualiser l'arborescence des utilisateurs *Commande* : tree /home

```
[root@romain ~]# tree /home
/home
├── lost+found
└── romain
    └── Documents

3 directories, 0 files
[root@romain ~]#
```

Question 5 : Créer le répertoire de la mission *Commande* : mkdir /home/mission_banque

```
[root@romain ~]# mkdir /home/mission_banque
[root@romain ~]# ls /home
mission_banque  lost+found  romain
[root@romain ~]#
```

Question 6 : Se déplacer dans le dossier créé *Commande* : cd /home/mission_banque

```
[root@romain ~]# cd /home/mission_banque
[root@romain mission_banque]# pwd
/home/mission_banque
[root@romain mission_banque]#
```

Question 7 : Créer le fichier vide *Commande* : touch logs.txt

```
[root@romain mission_banque]# touch logs.txt
[root@romain mission_banque]# ls
logs.txt
[root@romain mission_banque]#
```

Question 8 : Vérifier le contenu après édition (vim) Commande : cat logs.txt

```
[root@romain mission_banque]# cat logs.txt
Audit_Demarré=Vrai
[root@romain mission_banque]#
```

Question 9 : Faire une copie de sauvegarde Commande : cp logs.txt logs.bak

```
[root@romain mission_banque]# cp logs.txt logs.bak
[root@romain mission_banque]# ls
logs.bak  logs.txt
[root@romain mission_banque]#
```

Question 10 : Renommer le fichier original Commande : mv logs.txt rapport_final.log

```
[root@romain mission_banque]# mv logs.txt rapport_final.log
[root@romain mission_banque]# ls
logs.bak  rapport_final.log
[root@romain mission_banque]#
```

Question 11 : Supprimer la copie inutile Commande : rm logs.bak

```
[root@romain mission_banque]# rm logs.bak
[root@romain mission_banque]# ls
rapport_final.log
[root@romain mission_banque]#
```

Question 12 : Créer l'utilisatrice Johanne Commande : useradd johanne

```
[root@romain mission_banque]# useradd johanne
[root@romain mission_banque]# grep johanne /etc/passwd
johanne:x:1001:1001::/home/johanne:/bin/sh
[root@romain mission_banque]#
```

Question 13 : Attribuer un mot de passe Commande : passwd johanne

```
[root@romain mission_banque]# passwd johanne
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
[root@romain mission_banque]#
```

Question 14 : Créer le groupe "auditeurs" Commande : groupadd auditeurs

```
[root@romain mission_banque]# groupadd auditeurs
[root@romain mission_banque]# grep auditeurs /etc/group
auditeurs:x:1002:
[root@romain mission_banque]#
```

Question 15 : Ajouter l'utilisatrice au groupe *Commande* : usermod -aG auditeurs johanne

```
[root@romain mission_banque]# usermod -aG auditeurs johanne
[root@romain mission_banque]# groups johanne
johanne : johanne auditeurs
[root@romain mission_banque]#
```

Question 16 : Changer le propriétaire du fichier *Commande* : chown johanne rapport_final.log

```
[root@romain mission_banque]# chown johanne rapport_final.log
[root@romain mission_banque]# ls -l rapport_final.log
-rw-r--r-- 1 johanne root 19 janv. 10:05 rapport_final.log
[root@romain mission_banque]#
```

Question 17 : Changer le groupe du fichier *Commande* : chgrp auditeurs rapport_final.log

```
[root@romain mission_banque]# chgrp auditeurs rapport_final.log
[root@romain mission_banque]# ls -l rapport_final.log
-rw-r--r-- 1 johanne auditeurs 19 janv. 10:05 rapport_final.log
[root@romain mission_banque]#
```

Question 18 : Sécuriser les permissions (640) *Commande* : chmod 640 rapport_final.log

```
[root@romain mission_banque]# chmod 640 rapport_final.log
[root@romain mission_banque]#
```

Question 19 : Vérifier les droits finaux *Commande* : ls -l rapport_final.log

```
[root@romain mission_banque]# ls -l rapport_final.log
-rw-r----- 1 johanne auditeurs 19 janv. 10:05 rapport_final.log
[root@romain mission_banque]#
```

Question 20 : Compresser/Sauvegarder le dossier de travail *Commande* : tar -czvf

```
[root@romain mission_banque]# tar -czvf mission.tar.gz /home/mission_banque
tar: Suppression de « / » au début des noms des membres
/home/mission_banque/
/home/mission_banque/rapport_final.log
[root@romain mission_banque]# ls *.gz
mission.tar.gz
[root@romain mission_banque]#
```

Conclusion

En conclusion, ce TP nous a permis de pratiquer les commandes de base de l'administration Linux. Nous avons appris à créer et organiser des fichiers, gérer les utilisateurs et sécuriser les données. Ce travail aide à mieux comprendre le rôle d'un administrateur système et l'importance de la sécurité informatique.